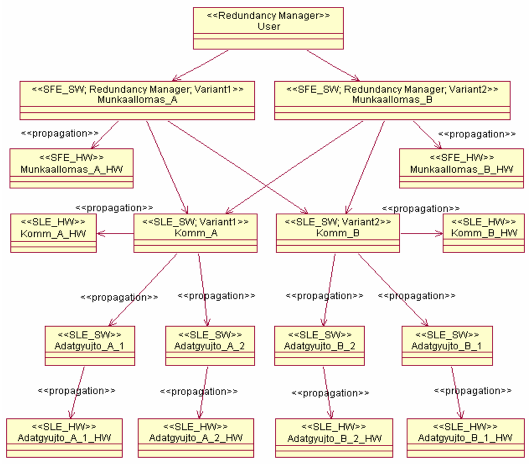
Dependability Analysis

Design and Integration of Embedded Systems

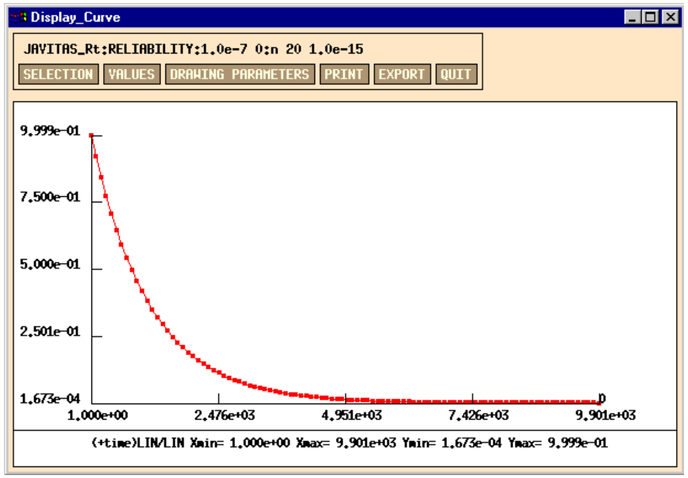
István Majzik

Department of Measurement and Information Systems

Goals



<<Redundancy Manager>>
User
<<SFE_SW; Redundancy Manager; Variant1>>
Munkaallomas_A
<<SFE_SW; Redundancy Manager; Variant2>>
Munkaallomas_B
<<propagation>>
<<SFE_HW>>
Munkaallomas_A_HW
<<SFE_HW>>
Munkaallomas_B_HW
<<SLE_HW>>
Komm_A_HW
<<SLE_SW; Variant1>>
Komm_A
<<SLE_SW; Variant2>>
Komm_B
<<SLE_HW>>
Komm_B_HW
<<SLE_SW>>
Adatgyujto_A_1
<<SLE_SW>>
Adatgyujto_A_2
<<SLE_SW>>
Adatgyujto_B_2
<<SLE_SW>>
Adatgyujto_B_1
<<SLE_HW>>
Adatgyujto_A_1_HW
<<SLE_HW>>
Adatgyujto_A_2_HW
<<SLE_HW>>
Adatgyujto_B_2_HW
<<SLE_HW>>
Adatgyujto_B_1_HW



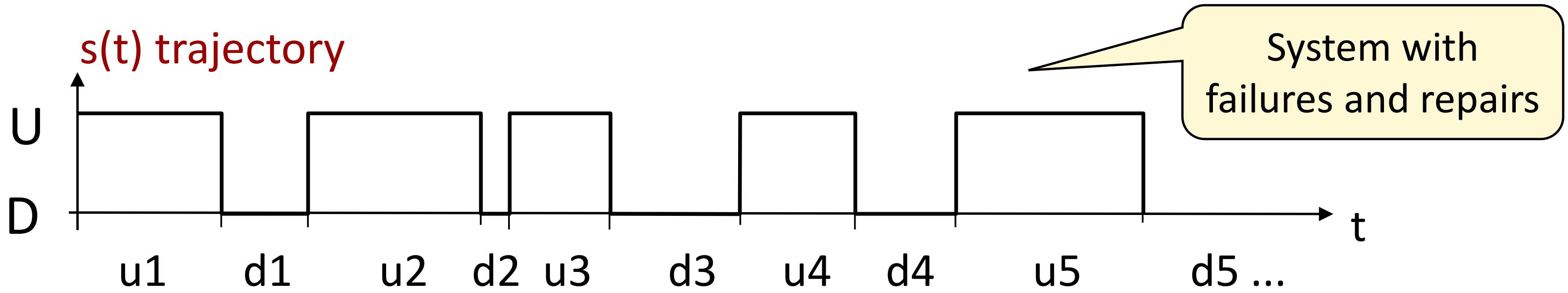
Display_Curve
JAVITAS_Rt:RELIABILITY:1.0e-7 0:n 20 1.0e-15
SELECTION
VALUES
DRAWING PARAMETERS
PRINT
EXPORT
QUIT
9.999e-01
7.500e-01
5.000e-01
2.501e-01
1.673e-04
1.000e+00
2.476e+03
4.951e+03
7.426e+03
9.901e+03
(+time)LIN/LIN Xmin= 1.000e+00 Xmax= 9.901e+03 Ymin= 1.673e-04 Ymax= 9.999e-01

Overview: Analysis techniques

- Recap: Qualitative analysis techniques
  - Fault effects analysis: What are the component level faults, that cause system level failure?
    - Identification of single points of failure
    - Calculation of system hazard probabilities
  - Techniques: Systematic analysis of faults and their effects
    - Fault tree analysis (FTA), Event tree analysis (ETA), Cause-consequence analysis (CCA), Failure modes and effects analysis (FMEA)
- Quantitative analysis techniques
  - Dependability analysis: How can the system level dependability be calculated on the basis of component level fault rates?
    - Calculation of system level reliability, availability, safety, MTTF
  - Techniques: Construction and solution of dependability models
    - Reliability block diagrams (RBD)
    - Markov-chains (MC)

Recap: System level dependability metrics (1)

- Basis: Partitioning the states of the system s(t)
  - Correct (U, up) and incorrect (D, down) state partitions



- Mean values:
  - Mean Time to First Failure: MTFF = E{u1}
  - Mean Up Time: MUT = MTTF = E{ui}
    (Mean Time To Failure)
  - Mean Down Time: MDT = MTTR = E{di}
    (Mean Time To Repair)
  - Mean Time Between Failures: MTBF = MUT + MDT

Recap: System level dependability metrics (2)

- Probability functions:
  - Availability:

    $a(t) = P\{ s(t) \in U \}$ (failures and repairs are possible)
  - Reliability:

    $r(t) = P\{ s(t') \in U, \forall t'<t\}$ (continuous fault-free operation)

Probability function for safety:
Probability of being in the
safe state partition

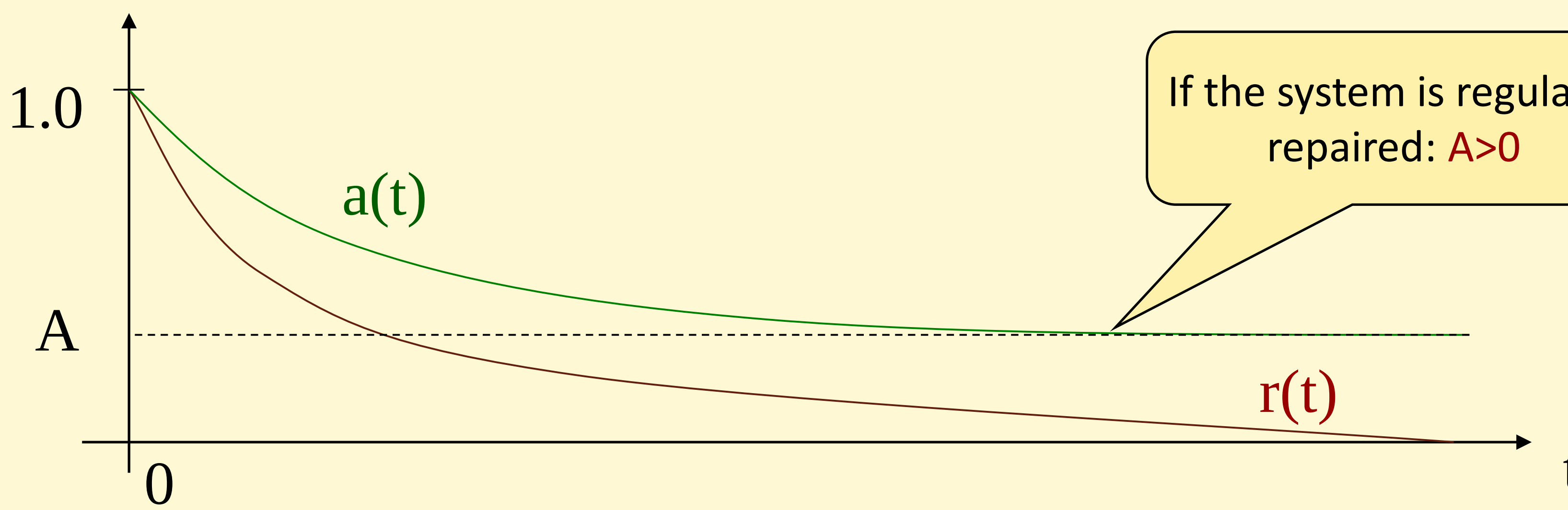
- Asymptotic values:
  - Asymptotic availability:

$$A = \lim_{t\to\infty} a(t)$$

$$A = \frac{\text{MUT}}{\text{MUT+MDT}} = \frac{\text{MTTF}}{\text{MTTF+MTTR}}$$

Recap: System level dependability metrics (2)

- Probability functions:
  - Availability:
    a(t) = P{ s(t) ∈ U } (failures and repairs are possible)
  - Reliability:
    r(t) = P{ s(t’) ∈ U, ∀t’<t} (continuous fault-free operation)



Recap: Component fault rate

- Fault rate: $\lambda(t)$

Probability that the component will fail in the interval Δt at time point t given that it has been correct until t is given by λ(t)Δt

$$\lambda(t)\Delta t = P\left\{s(t+\Delta t)\in D \mid s(t)\in U\right\} \text{ while } \Delta t \to 0$$

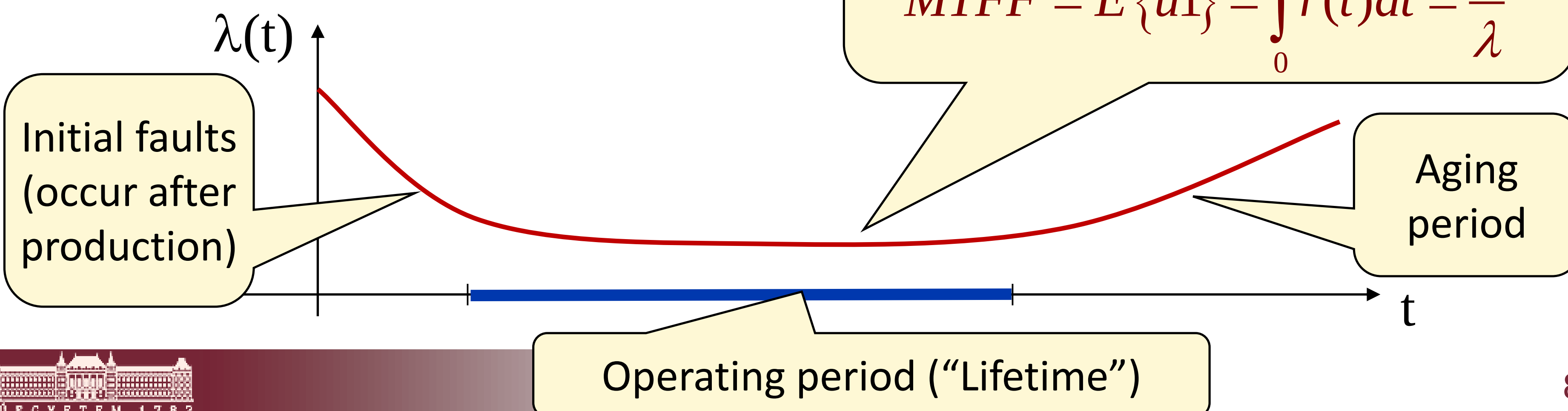
- Reliability of a component on the basis of this definition:

$$r(t) = e^{-\int_0^t \lambda(t)\,dt}$$

- For electronic components:

Here $r(t) = e^{-\lambda t}$

$$MTFF = E\{u1\} = \int_0^\infty r(t)\,dt = \frac{1}{\lambda}$$

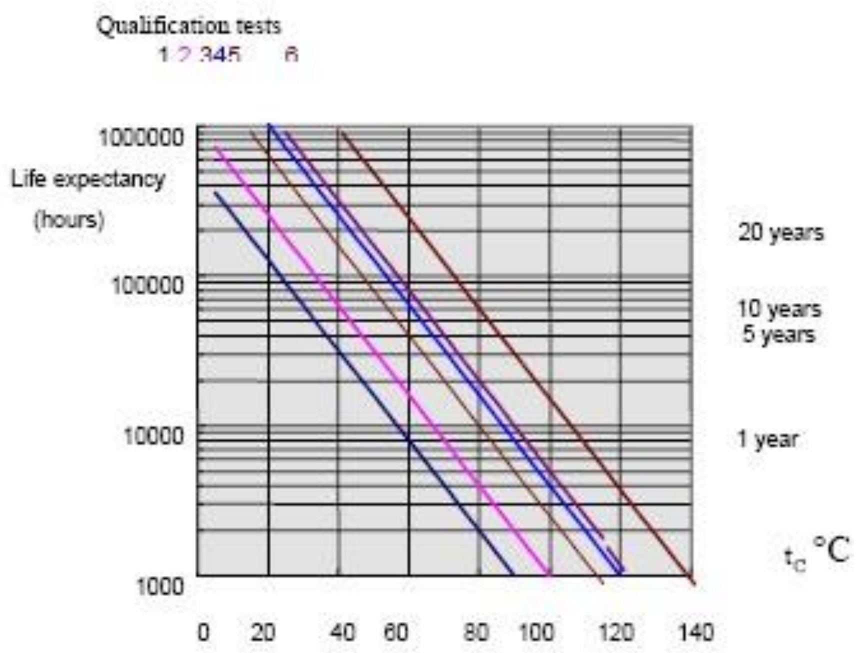


How to estimate component fault rate?

- Component level fault rates are available in handbooks
  - MIL-HDBK-217: The Military Handbook – Reliability Prediction of Electronic Equipment (for military applications, pessimistic)
  - Telcordia SR-332: Reliability Prediction Procedure for Electronic Equipment (for telco applications)
  - IEC TR 62380: Reliability Data Handbook - Universal Model for Reliability Prediction of Electronic Components, PCBs, and Equipment (less pessimistic, supporting new component types)
- Dependencies of component fault rate
  - Temperature, weather conditions, shocking (e.g., in vehicles), altitude, …
  - Operational profiles
    - Ground; stationary; weather protected (e.g., in rooms)
    - Ground; non stationary; moderate (e.g., in vehicles)

How to estimate lifetime?

- Important to estimate lifetime of electronic components
  - When does the fault rate start increasing?
  - At this time scheduled maintenance (replacement) is required
- IEC 62380: „Life expectancy” is defined
- Example: Life expectancy of electrolyte capacitors
  - Depends on temperature
  - Depends on qualification
  - Example: at 25°C,
    ~ 100 000 hours (~ 11 years)



Goals of the dependability analysis

- On the basis of component characteristics like
  - fault rate (in continuous operation), measured by FIT: 1 FIT = 10^{-9} faults/hour
  - fault probability (in on-demand operation)
  - reliability function,

  calculation of system level characteristics like
  - reliability function
  - availability function
  - safety function
  - asymptotic availability
  - MTTF, MTFF, MTBF

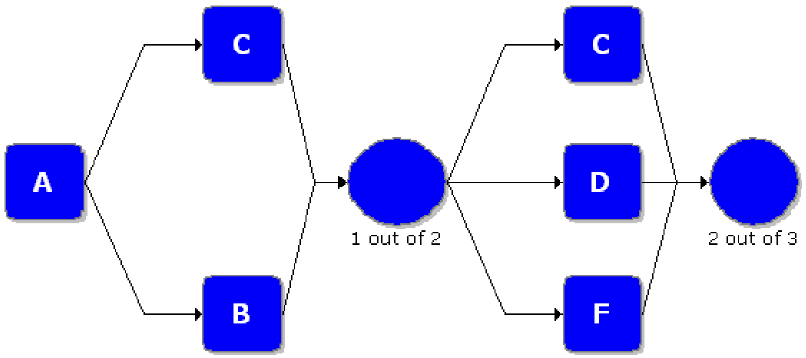
Calculations are based on the system architecture (redundancy structures) and the failure modes

Calculations related to hazardous faults (faults that are safe are not considered)

Using the results of the analysis

- Design: Comparison of alternative architectures
  - Having the same components, which architecture guarantees better dependability attributes?
- Design, maintenance: Sensitivity analysis
  - What are the effects of selecting another component?
  - Which components have to be changed in case of inappropriate system level characteristics?
  - Which component characteristics have to be investigated in more detail? → Fault injection and measurements
- Delivery: Justification of dependability attributes
  - Approval of systems
  - Certification (by safety authority)

Combinatorial models for dependability analysis



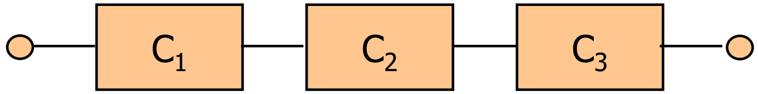
Boole-models for calculating dependability

- Two states of components: Fault-free or faulty
- There are no dependencies among the components
  - Neither from the point of view of fault occurrences
  - Nor from the point of view of repairs
- "Interconnection" of components from the point of view of dependability: What kind of redundancy is used?
  - Serial connection: The components are not redundant
    - All components are necessary for the system operation
  - Parallel connection: The components are redundant
    - The components may replace each other
  - Connection scheme may depend on the component failure mode

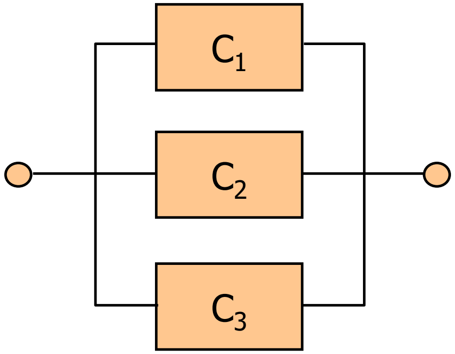
Reliability block diagram

- Blocks: Components (with failure modes)
- Connection: Serial or parallel (w.r.t. redundancy)
- Paths: System configurations
  - The system is operational (correct) if there is a path from the start point to the end point of the reliability block diagram through fault-free components

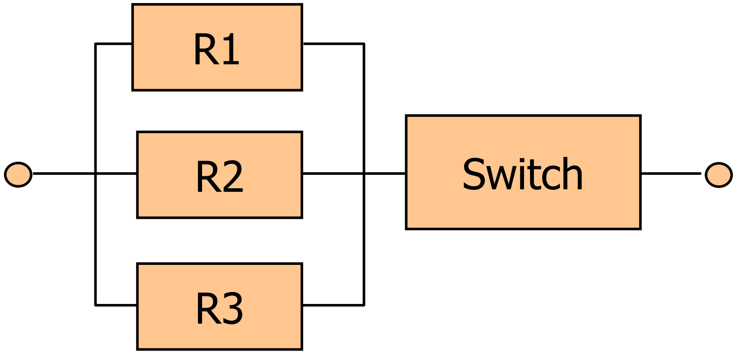
Serial connection:

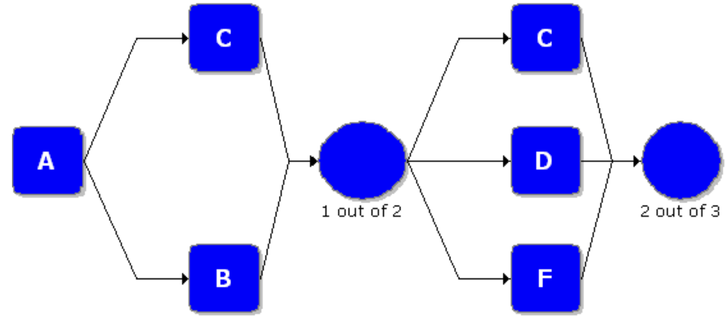


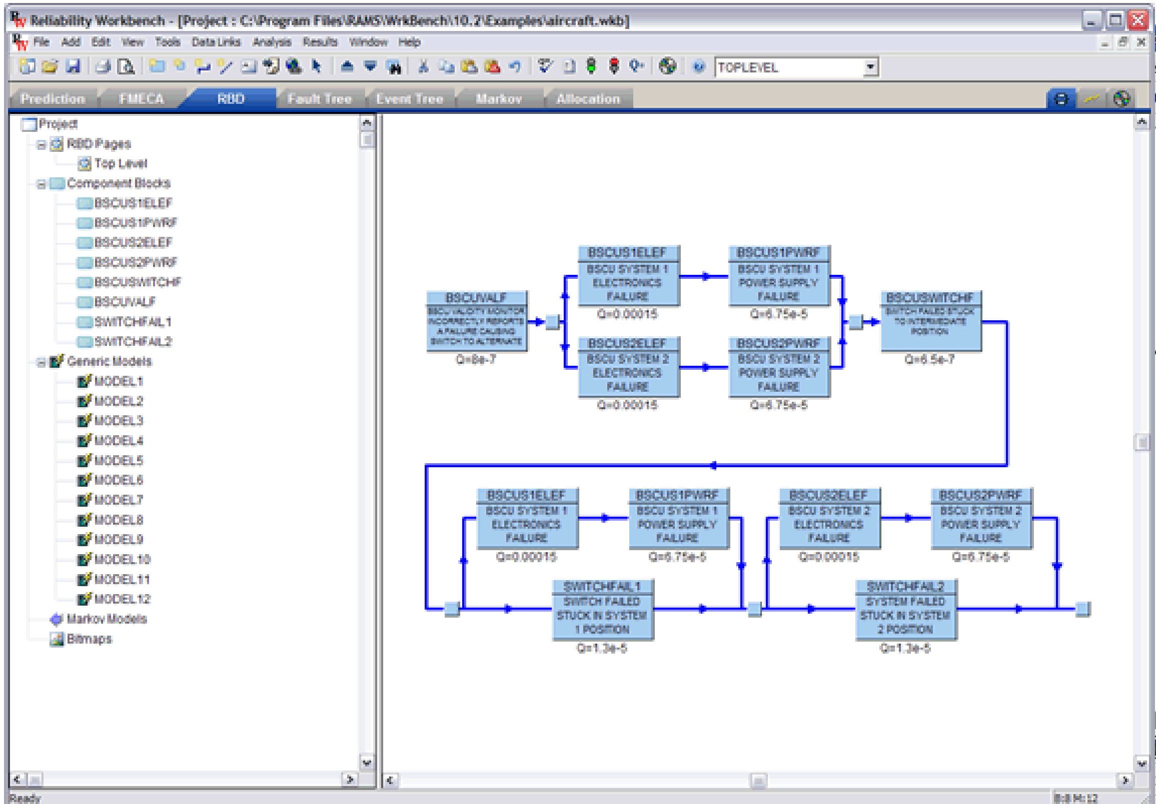
Parallel:

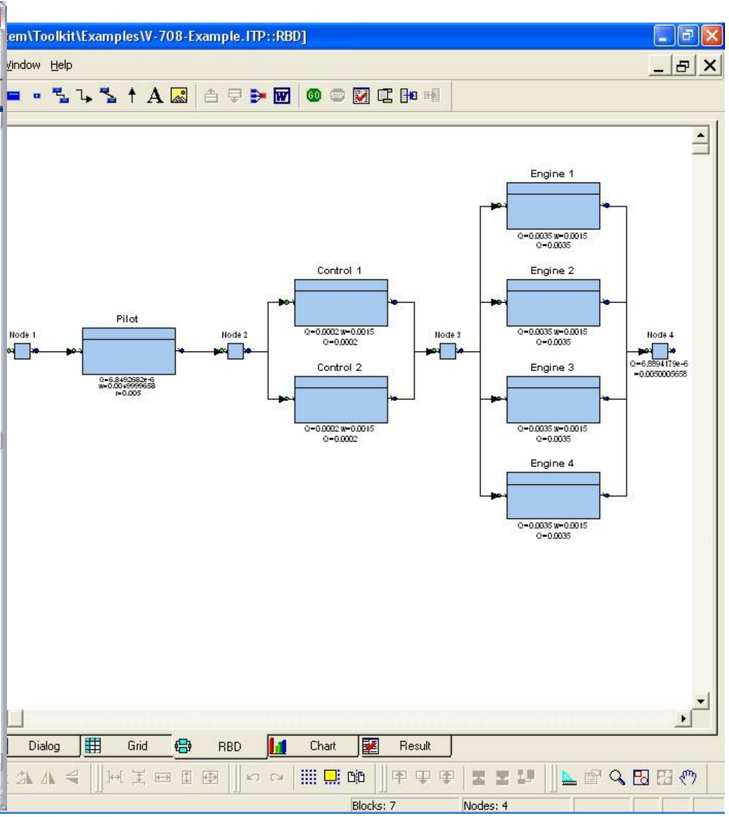


Reliability block diagram examples



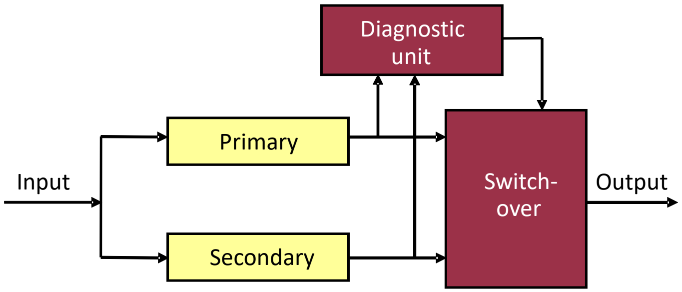




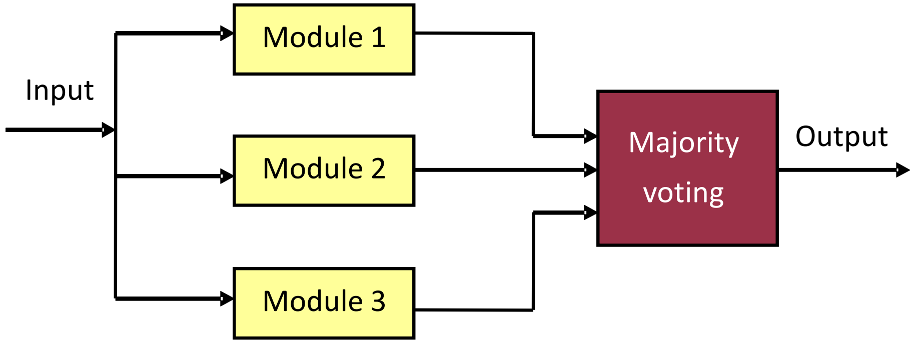


Overview: Typical system configurations

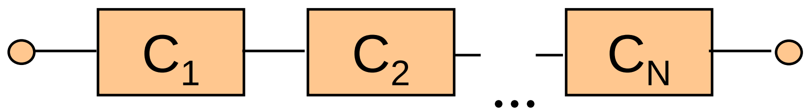
- Serial system model: No redundancy
- Parallel system model: Redundancy (replication)

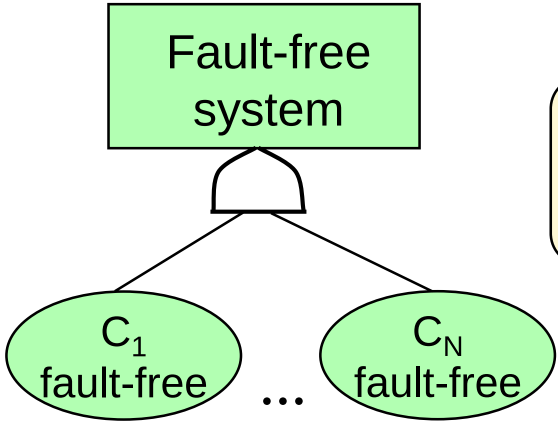


- Canonical system: Serial and parallel subsystems
- M out of N components: Majority voting (TMR)



Serial system model





P(A∧B)=P(A)·P(B)
if independent

- Reliability for N serial components:

$$r_R(t) = \prod_{i=1}^{N} r_i(t)$$

System reliability

Components' reliability

$$r(t) = e^{-\lambda t}$$

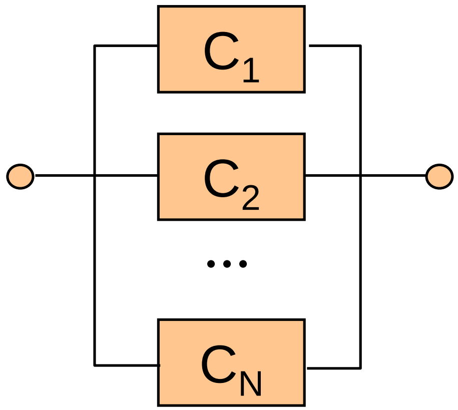
$$\lambda_R = \sum_{i=1}^{N} \lambda_i$$

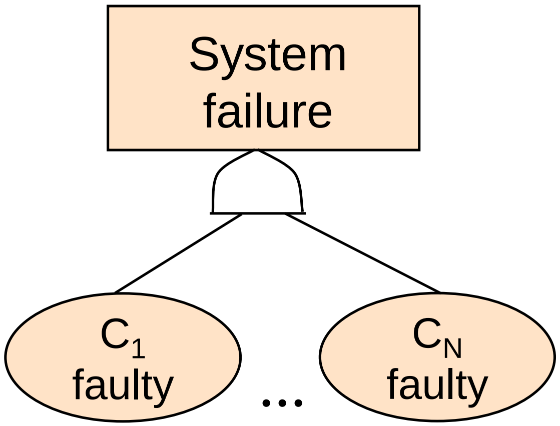
- MTFF:

$$MTFF = \frac{1}{\lambda}$$

$$MTFF = \frac{1}{\sum_{i=1}^{N} \lambda_i}$$

Parallel system model





P(A∧B)=P(A)·P(B)
if independent

- Reliability:

$$1 - r_R(t) = \prod_{i=1}^{N} (1 - r_i(t))$$

- Identical N components:

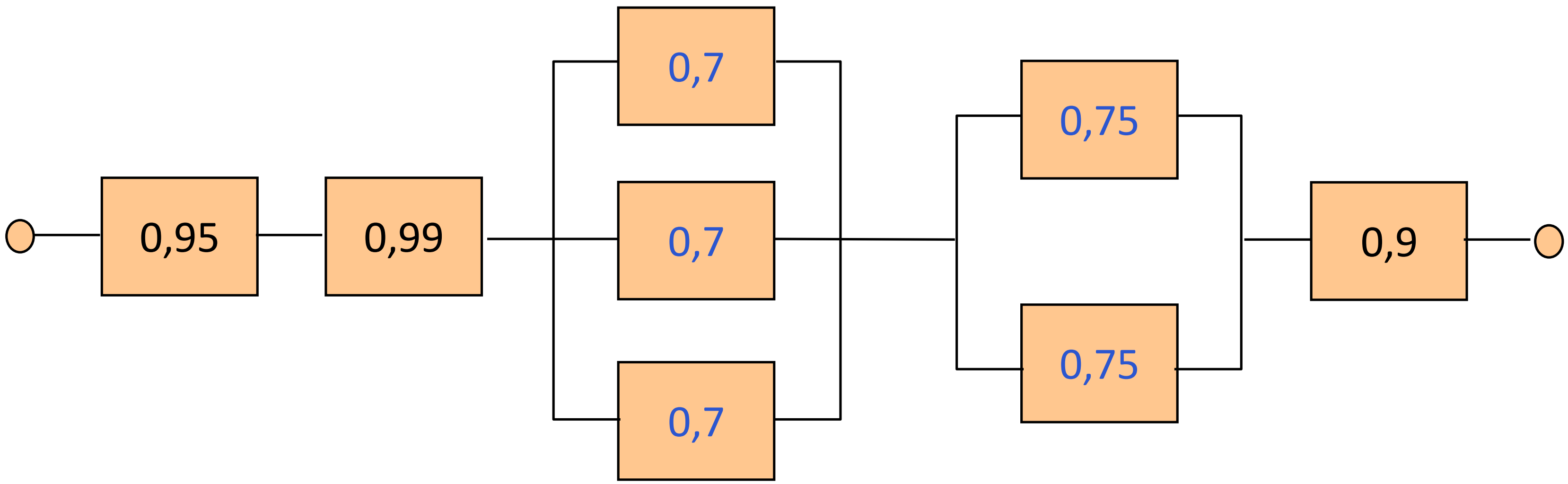
$$r_R(t) = 1 - (1 - r_C(t))^N$$

- MTFF:

$$MTFF = \frac{1}{\lambda} \sum_{i=1}^{N} \frac{1}{i}$$

Complex canonical system

- Subsystems with serial or parallel components
- Example: Calculation of asymptotic availability



- System level asymptotic availability:

$$A_R = 0,95 \cdot 0,99 \cdot \left[1-\left(1-0,7\right)^3\right] \cdot \left[1-\left(1-0,75\right)^2\right] \cdot 0,9$$

M faulty out of N components

- N replicated components;
  If M or more components are faulty: the system is faulty

$$r_R = \sum_{i=0}^{M-1} P\{\text{"there are i faulty components"}\}$$

$$r_R = \sum_{i=0}^{M-1} \binom{N}{i} (1-r)^i \cdot r^{N-i}$$

Here component reliability is denoted in short by r instead of r(t)

- Applied for: Majority voting (TMR): N=3, M=2

$$r_R = \sum_{i=0}^{1} \binom{3}{i} (1-r)^i \cdot r^{3-i} = \binom{3}{0} (1-r)^0 \cdot r^3 + \binom{3}{1} (1-r)^1 \cdot r^2 = 3r^2 - 2r^3$$

$$MTFF = \int_0^\infty r_R(t)dt = \int_0^\infty (3r^2 - 2r^3)dt = \frac{5}{6} \cdot \frac{1}{\lambda}$$

Less than in case of a single component!

But $r_R(t)$ is higher than r(t) between t=0 and 0.7/λ → survival of a mission time

TMR/simplex system

- Basic case: TMR operation
- In case of fault: Switchover to simplex (single component) configuration
  - The voter identifies the faulty component
  - One of the non-faulty components is selected to be operated as a simplex system
    (possibly with fault detection by comparison with the other)

$$MTFF = \frac{4}{3} \cdot \frac{1}{\lambda}$$

$$r_R = \frac{3}{2} r - \frac{1}{2} r^3$$

Cold redundant system

- In case of a fault of the primary component a redundant component is switched on to replace the primary:

$$MTFF = \sum_{i=1}^{N} MTFF_i$$

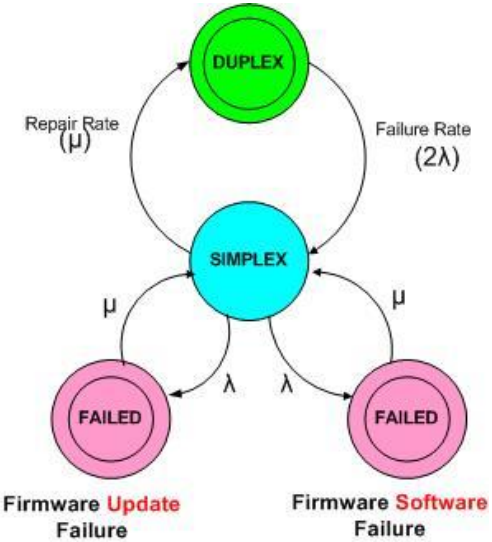
- In case of identical replicated components, the system reliability function:

$$r_R(t) = \sum_{i=0}^{N-1} \frac{(\lambda t)^i}{i!} e^{-\lambda t}$$

Summary

- Reliability block diagrams
- Boole-models for canonical systems
  - Serial
  - Parallel
  - M faulty out of N, TMR
  - Cold redundancy
- Comparison of architectures and dependence on component quality

Markov models for dependability analysis

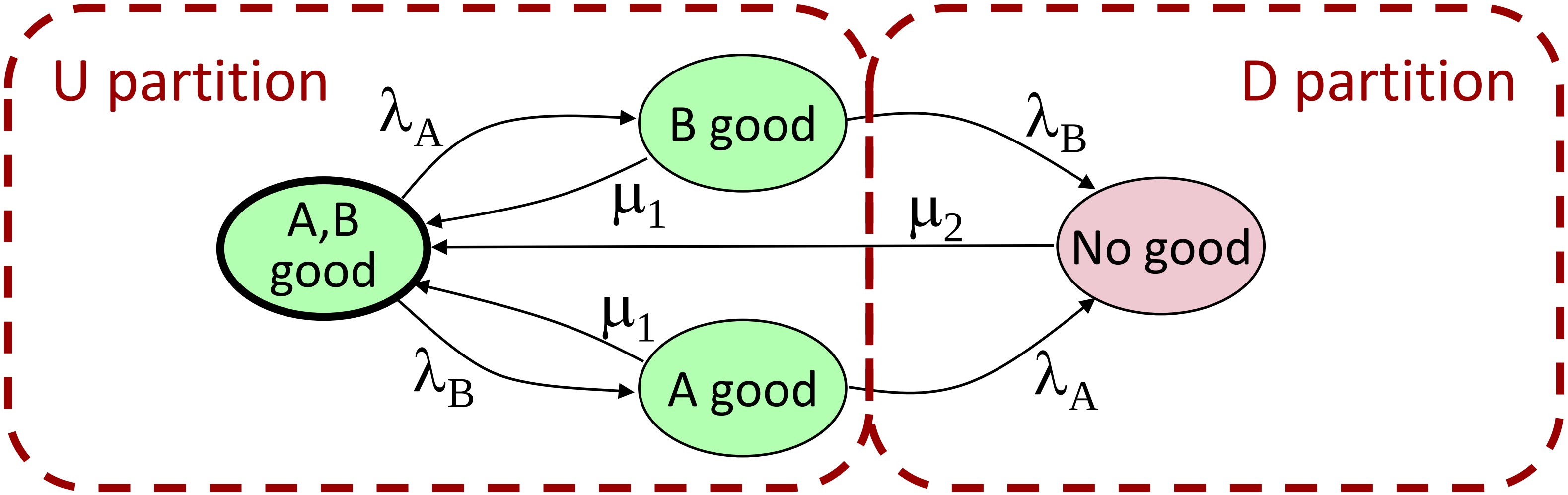


Modelling with Markov chains

- Elements of the Markov models
  - States ← Combinations of the faulty / fault-free states of components
  - Transitions ← Component fault occurrence or repair
  - Transition rates ← Component fault rate or repair rate (repair rate: reciprocal of repair time)
- Analysis of Markov models
  - Transient: Computing probability time functions of states
  - Steady-state: Computing the asymptotic probabilities of states (as time approaches infinity)
- Availability analysis at system level
  - Sum of the transient / steady-state probabilities of states in the U state partition

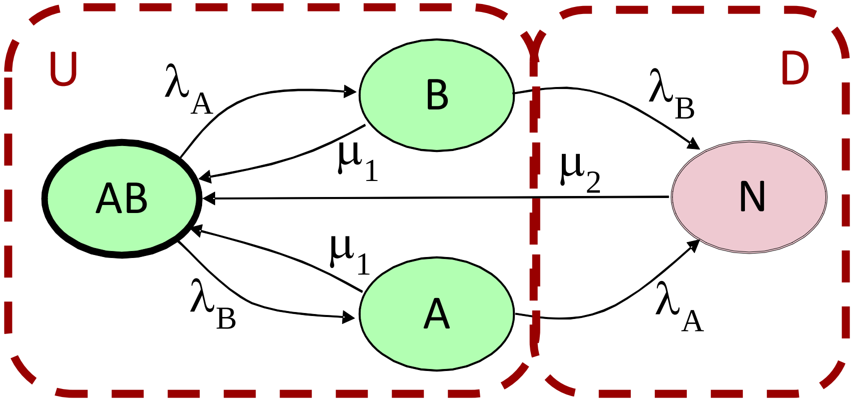
Example: CTMC dependability model (1)

- System consisting of two servers, A and B:
  - The servers may independently fail
  - The servers can be repaired independently or together
- Transition rates:
  - Fault of server A: λ_A fault rate
  - Fault of server B: λ_B fault rate
  - Repair of a server: μ_1 repair rate
  - Repair of both servers: μ_2 repair rate
- System states: Combination of the server states (good/faulty)



Example: CTMC dependability model (2)

- State partitions (with simplified state names):
  - $U = \{s_{AB}, s_A, s_B\}$
  - $D = \{s_N\}$
- State probabilities computed:
  - Transient: $\pi(s_i, t)$
  - Steady-state: $\pi(s_i)$



- Availability:

$$a(t) = \pi(s_{AB}, t) + \pi(s_A, t) + \pi(s_B, t)$$

- Asymptotic availability:

$$A = \pi(s_{AB}) + \pi(s_A) + \pi(s_B)$$

- Reliability calculation:
  - The model shall be modified: transitions from partition D to U shall be deleted (no system repair)
  - Reliability calculated in this model:

$$r(t) = \pi(s_{AB}, t) + \pi(s_A, t) + \pi(s_B, t)$$